DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 4, 7, 12, and 52

[FAC 2005-88; FAR Case 2011-020; Item III; Docket No. 2011-0020, Sequence No. 1]

RIN 9000-AM19

Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems

AGENCIES: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Final rule.

SUMMARY: DoD, GSA, and NASA are issuing a final rule amending the Federal Acquisition Regulation (FAR) to add a new subpart and contract clause for the basic safeguarding of contractor information systems that process, store or transmit Federal contract information. The clause does not relieve the contractor of any other specific safeguarding requirement specified by Federal agencies and departments as it relates to covered contractor information systems generally or other Federal requirements for safeguarding Controlled Unclassified Information (CUI) as established by Executive Order (E.O.). Systems that contain classified information, or CUI such as personally identifiable

information, require more than the basic level of protection.

DATES: Effective: [**Insert date 30 days after publication in the FEDERAL REGISTER**].

FOR FURTHER INFORMATION CONTACT: Ms. Cecelia L. Davis, Procurement Analyst, at 202-219-0202, for clarification of content. For information pertaining to status or publication schedules, contact the Regulatory Secretariat Division at 202-501-4755. Please cite FAC 2005-88, FAR Case 2011-020.

SUPPLEMENTARY INFORMATION:

I. Background

This final rule has basic safeguarding measures that are generally employed as part of the routine course of doing business. DoD, GSA, and NASA published a proposed rule in the Federal Register at 77 FR 51496 on August 24, 2012, to address the safeguarding of contractor information systems that contain or process information provided by or generated for the Government (other than public information). This proposed rule had been preceded by DoD publication of an Advance Notice of Proposed Rulemaking (ANPR) and notice of public meeting in the Federal Register at 75 FR 9563 on March 3, 2010, under Defense Federal Acquisition Regulation Supplement (DFARS) Case 2008-D028,

Safeguarding Unclassified Information. The ANPR addressed basic and enhanced safeguarding procedures for the protection of DoD unclassified information. Resulting public comments on the DFARS rule were considered in drafting a proposed FAR rule under FAR case 2009-030, which focused on the basic safeguarding of unclassified Federal information contained within information systems. On June 29, 2011, the contents of FAR case 2009-030 were merged into FAR case 2011-020, Basic Safeguarding of Contractor Information Systems.

This rule, which focuses on ensuring a basic level of safeguarding for any contractor system with Federal information, reflective of actions a prudent business person would employ, is just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems. Last summer, OMB issued proposed guidance to enhance and clarify cybersecurity protections in Federal acquisitions related to CUI in systems that contractors operate on behalf of the Government as well as in systems that are not operated on behalf of an agency but are used incidental to providing a product or service for an agency with particular focus on security controls, incident reporting, information system assessments, and information security continuous

monitoring. DOD, GSA, and NASA will be developing FAR changes to implement the OMB guidance when it is finalized.

In addition, we plan to develop regulatory changes for the FAR in coordination with National Archives and Records Administration (NARA) which is separately finalizing a rule to implement E.O. 13556 addressing CUI. The E.O. established the CUI program to standardize the way the executive branch handles information (other than classified information) that requires safeguarding or dissemination controls.

All of these actions should help, among other things, clarify the application of the Federal Information Security Management Act (FISMA) and the National Institute of Standards and Technology (NIST) information systems requirements to contractors and, by doing so, help to create greater consistency, where appropriate, in safeguarding practices across agencies. Prior to all of these actions occurring, DOD has updated a DFARS rule addressing enhanced safeguarding for certain sensitive DOD information in those systems.

Sixteen respondents submitted comments on this proposed rule.

II. Discussion and Analysis

The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (the Councils) reviewed the comments in the development of the final rule. A discussion of the comments and the changes made to the rule as a result of those comments are provided as follows:

A. Summary of significant changes from the proposed rule.

1. Safeguarding of covered contractor information system.

- Provides for safeguarding the contractor information system, rather than specific information contained in the system.

- Revises the title of the case and throughout the final rule to add the term "covered" to "contractor information system," thus indicating that the policy applies only to contractor information systems that contain Federal contract information.

2. Safeguarding requirements.

- Deletes the safeguarding requirements and procedures in the clause that relate to transmitting electronic information, transmitting voice and fax information, and information transfer limitations.

- Replaces the other safeguarding requirements with comparable security requirements from NIST SP 800-171.

3. Definitions.

- Adds definitions of "covered contractor information system" and "Federal contract information."
- Deletes definitions of "public information" and all other proposed definitions in the clause, except "information," "information system," and "safeguarding."

4. Applicability. Makes the final rule—

- Applicable below the simplified acquisition threshold.
- Not applicable to the acquisition of commercially available off-the-shelf (COTS) items.

5. Other safeguarding requirements. Clarifies that the clause does not relieve the contractor from complying with any other specific safeguarding requirements and procedures specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal requirements for safeguarding CUI as established by E.O. 13556.

B. Analysis of public comments.

1. Scope and applicability.

a. Information provided by or generated for the Government (other than public information).

Comments: About half the respondents commented on the scope and applicability of the proposed rule, which required safeguarding of information provided by or generated for the Government (other than public information). The proposed rule included the statutory definition of "public information" from 44 U.S.C. 3502. The respondents generally commented on the breadth of the scope or a lack of clarity.

One respondent urged the FAR Council to withhold release of a final rule until NARA implements E.O. 13556, Controlled Unclassified Information. Without such coordination, contractors may be required to establish conflicting protections that may later conflict or be revised by the Governmentwide NARA program.

Several respondents were also concerned about the broad potential scope of the information subject to these requirements. One respondent stated that the rule would cover nearly all information and all information systems of any company that holds even a single Government contract. One respondent questioned whether "generated for the Government" just applied to information that is part of a contract deliverable, or whether it also covered

information about the contractor's own proprietary practices that is submitted to the Government. Another respondent was concerned that agencies have tended to broadly expand FISMA requirements to information developed under Federal contracts, regardless of whether the information is a deliverable under the contract (e.g., data exchanged among researchers). One respondent recommended limiting the covered information to "information provided by or delivered to the Government." Another respondent urged narrowing the rule to the type of information for which safeguards are warranted, based on a reasoned risk assessment and cost-benefit analysis. One respondent recommended that the rule should exclude contractor proprietary or trade secret data from the scope of information generated for the Government, so that the responsibility for protecting such information remains with the contractor.

One respondent is concerned that the Government may send non-public information to a recipient, who may be unaware that it is in their possession on any device, in any form. The information could be temporarily exposed, even if transferred and not retained.

Further, respondents were concerned about interpretation of the definition of "public information."

Several respondents considered that the definition of "public information" was too narrow, because it requires the actual disclosure, dissemination, or disposition of information. One respondent stated that the Government has significant volumes of data that have not yet been made public, but that may be subject to obligations for disclosure under a variety of statutes. Several respondents stated that contractors cannot readily determine what information is categorized as public information, because it is almost impossible for contractors to keep track of what information has been released to the public.

One respondent stated that the Government should proactively mark protected materials.

Response: The intent is that the scope and applicability of this rule be very broad, because this rule requires only the most basic level of safeguarding. However, applicability of the final rule is limited to covered contractor information systems, i.e., systems that are owned or operated by a contractor that process, store, or transmit Federal contract information. "Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product

or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments. The final rule has been coordinated with NARA. The focus of the final rule is shifted from the safeguarding of specific information to the basic safeguarding of certain contractor information systems. Therefore, it is not necessary to draw a fine line as to what information was "generated for the Government," when the information is received, or whether the information is marked. The requirements pertain to the information system itself. The type of analysis required to narrow the rule to the type of information for which safeguards are warranted, based on risk-assessment and cost-benefit analysis, is appropriate for CUI and the enhanced safeguarding that would be required for such information consistent with law, Federal regulation, and Governmentwide policy. A prudent business person would employ this most basic level of safeguarding, even if not covered by this rule. This rule is intended to provide a basic set of protections for all Federal contract information, upon which other rules, such as a forthcoming FAR rule to protect CUI, may build.

Since the safeguarding applies to the contractor information system, not to specific information within the system, it is irrelevant whether there is also contractor information in the system. However, if the contractor stores pre-existing proprietary data or trade secrets in a separate information system, the contractor can decide how to protect its own information.

The definition of "public information" has been deleted, as it is no longer necessary.

b. Information residing in or transiting through a contractor information system.

Comment: One respondent requested clarification of the statutory definition of "information system," i.e., what would be the limitation for a system interfacing with another system. The respondent requested that the rule specifically identify the medium of communication, the mechanism for delivering the communication, and the disposition.

Response: Generally, separately accredited information systems that interface through loosely coupled mechanisms, such as e-mail or Web services, are not considered direct connections, even if they involve dynamic interaction between software systems in different organizations that are designed to interact with each other

(e.g., messaging, electronic commerce/electronic data interchange transactions). It would not be practical to specify all the possible mechanisms for interaction among systems, since they are constantly evolving.

Comment: Another respondent requested a definition of "resides on or transits through" an information system. The respondent is concerned that much of the focus of information security efforts is directed at protecting perimeter devices and may overlook the necessity of protecting the host servers.

Response: Information "residing on" a system means information being processed by or stored on the information system. "Transiting through" the system means simple transport of the data through the system to another destination (i.e., no local storage or processing). All of the controls listed are focused on protection of the information system (e.g., the host servers, workstations, routers). None of the controls are devoted to protection of "perimeter devices" although several (particularly paragraphs (b)(1)(x) and (xi)) are applied at the perimeter of the system.

c. Solicitations.

Comment: One respondent was concerned that the requirements of the rule were applied to solicitations,

thus imposing this requirement as a barrier to even bidding on Government work. Another respondent commented that the FAR rule would affect not only companies that receive Government contracts, but also companies soliciting Government contracts.

Response: This was not the intent of the proposed rule. The final rule has revised the applicability section to address "acquisitions" rather than "solicitations and contracts." Of course, the clause prescription still requires inclusion of the clause in solicitations, so that offerors are aware of the clause that will be included in the resultant contract. The clause does not take effect until the offeror is awarded a contract containing the clause.

d. Fundamental research.

Comment: Two respondents requested exclusion of contracts for fundamental research from the requirements of the rule. One respondent noted that the prior proposed DFARS rule included an exception for solicitations and contracts for fundamental research, while also noting that most of the respondent's member institutions have at least first level information technology security measures in place within their systems, which appear to meet most of the basic safeguarding requirements. Another respondent,

while recognizing that some level of protection should be afforded, seeks regulations that will provide an appropriate level of protection without creating unwieldy compliance burdens or creating a chilling effect on academic activity, including fundamental research.

Response: The final rule does not focus on the protection of any specific type of information, but requires basic elements for safeguarding an information system. These requirements should not have any chilling effect on fundamental research.

e. Policies and procedures.

Comment: One respondent stated that the scope statement that the subpart provides policies and procedures is inaccurate, because the subpart just defines terms and prescribes the use of a contract clause.

Response: The scope section has been deleted in the final rule.

2. Basic safeguarding requirements.

a. General.

Comment: According to one respondent, some of the safeguarding requirements are too basic and rudimentary to achieve the rule's intended purpose.

Response: The intended purpose of the rule is to provide basic safeguarding of covered contractor

information systems. This rule is not related to any specific information categories other than the broad and basic safeguarding.

Comment: Various respondents were of the opinion that the rule should hold contractors to NIST and FISMA requirements.

- One respondent stated that the proposed rule severely downgrades existing recommendations in place by NIST regarding the proper procedures and controls for protection of Federal information systems. According to the respondent, the rule should require contractors to adhere to same standards required of Federal agencies by the NIST SP 800 x series and the FISMA.
- Another respondent noted that Federal agencies are required to adhere to information security standards and guidelines published by NIST in Federal Information Processing Standards (FIPS) and Special Publications (SP). These publications explicitly state that the same standards apply to outsourced external service providers. Agencies and their contractors are also required to implement the configuration control settings at a "bits and bytes" level contained in the security configuration control checklists found in the National

Security Program (NSP), which is co-hosted by NIST and the Department of Homeland Security (DHS).

Response: This rule establishes the basic, minimal information system safeguarding standards which Federal agencies are already required to follow internally and most prudent businesses already follow as well. The rule makes clear that Federal contractors whose information systems process, store, or transmit Federal contract information must follow these basic safeguarding standards. When contractors will be processing CUI or higher-level sensitive information, additional safeguarding standards, not covered by this rule will apply.

Comment: One respondent stated that the requirements are not specific enough from a technological standpoint to encompass the current state of information security technology.

Response: The final rule replaces the requirements in the proposed rule with requirements from NIST guidelines (NIST SP 800-171), which are appropriate to the level of technology, and are updated as technology changes. Flexibility is provided for specific implementation.

Comment: Another respondent recommended that the Councils should consider adopting a performance standard for protecting specific types of information from

unauthorized disclosure rather than the "design standard" in the proposed rule.

Response: The standards in the proposed rule and in the final rule are not design standards; they are performance standards.

Comment: One respondent requested clarification of the meaning of "safeguarding." According to the respondent, the definition of "safeguarding" neither refers to nor incorporates the definition of "information security." The respondent questions whether the rule intends to distinguish between information security and safeguarding.

Response: There is a basic distinction between "safeguarding" and "information security." "Safeguarding" is a verb and expresses required action and purpose. The term "safeguarding" is common in Executive orders relating to information systems. Although safeguarding has some commonality with "information security" the focus of information security is narrower. Safeguarding the contractor's information system will promote confidentiality and integrity of data, but is not specifically concerned with data availability.

Comment: One respondent recommended that the rule should just require the contractor to protect information

provided to or generated for the Government "at a level no less than what the company provides for its own confidential and proprietary business information."

Response: There would be no need for a FAR clause if that is all it required. That would provide no advantage over the current status. FISMA requires this protection of Federal contract information.

b. Specific requirements.

i. Protecting information on public computers or websites.

Comment: One respondent commented on the requirement in the proposed rule (FAR 52.204-21(b)(1)) to protect information on public computers or websites. The respondent recommended focusing on covered contractor information systems. If retaining the term "public computers," the respondent recommended defining the term, taking into consideration that some contractors have a contractual obligation to use "public computers" in performance of a contract, and removing the restriction on the use of public computers if the use has implemented a secure means of accessing the covered Government information.

Response: The heading in the proposed rule in FAR paragraph 52.204-21(b)(1), "Protecting information on

public computers or Web sites," misstated the intent of the requirement. The requirement was to not process information provided by the Government on public computers or websites. In the final rule, this heading has been removed and the requirement has been restated to be consistent with NIST 800-171.

ii. Transmitting electronic information.

Comment: Many respondents commented on the requirement in the proposed rule (FAR 52.204-21(b)(2)) regarding transmitting electronic information. The primary concern of all of these respondents was the requirement for "the best level of security and privacy available given facilities, conditions, and environment." As one respondent stated, this is not consistent with the objective of the rule to require basic safeguarding, is not a defined term of art, and may not be consistent with the cost-effective standards and risk-based approach established by FISMA. Another respondent noted that requiring contractors to use the best level for all data, would prevent businesses from upgrading communications security for the transmission of more sensitive data. Another respondent pointed out that changes in technology would cause frequent changes in what would constitute the

"best level." One respondent recommended replacing "best" with "adequate," or "commercially reasonable."

Response: After evaluating the public comments, the requirement regarding transmitting electronic information was removed from the coverage in the final rule because transmission of email, text messages, and blogs are outside the scope of the final rule, which deals with safeguards for the contractor's information system, not protection of information.

iii. Transmitting voice and fax information.

Comment: More than half the respondents commented on the requirement in the proposed rule (FAR 52.204-21(b)(3)) relating to transmitting voice and fax information. A primary concern of respondents was the requirement that covered information can be transmitted orally only when the sender has "reasonable assurance" that access is limited to authorized recipients. The respondents found this requirement to be too vague. According to one respondent, there is further concern that the term "voice information" could arguably apply to any oral communication, such as telephone conversations. One respondent recommended the adoption of strict, clear policies in securing the voice communications of contractor systems, including encryption requirements for all transmissions. One respondent

questioned whether the rule covered voice communication over CDMA [code-division multiple access], GSM [Global System for Mobile], and VOIP [voice-over-Internet-Protocol], or some combination of the three.

Response: After evaluation of public comments, the requirement regarding transmission by phone and fax are outside the scope of the final rule, which deals with safeguards for the contractor's information system not protection of information.

iv. Physical and electronic barriers.

Comment: Several respondents commented on the requirement in the proposed rule (FAR 52.204-21(b)(4)) regarding physical and electronic barriers to protect Federal contract information. There was general concern that for certain devices it would not be practicable to always have both a physical barrier and an electronic barrier, when not under direct individual control. One respondent was concerned that NIST does not mention the specific types of locks or keys that will provide acceptable protection. Another respondent questioned what "direct individual control" means. Another respondent was concerned about the potential need to protect the information itself, when in hard copy. One respondent considered that this requirement may philosophically

conflict with Government and commercial efforts to create and accommodate a mobile workforce.

Response: The requirements at FAR 52.204-21(b)(4) in the proposed rule have been replaced by multiple security controls in paragraph (b)(1) of the clause 52.204-21. There is no longer a specific requirement to have both a physical barrier and an electronic barrier in all instances. The rule now clearly addresses the protection of the information system as a whole, rather than just the protection of the Federal contract information. The requirement for a basic level of safeguarding for covered contractor information systems is not in philosophical conflict with accommodation of a mobile work force. For example, it is common practice not to leave a smart phone with access to Federal contract information unattended in a public place and without any password protection.

v. Sanitization.

Comment: One respondent commented on the requirement for data sanitization in the proposed rule (FAR 52.204-21(b)(5)). The respondent stated that the proposed rule did not adequately address data sanitization, because some media are unable to be cleared due to format or a lack of compatible equipment, and would require purging or

destruction for proper sanitization. The respondent also noted that the URL for NIST 800-88 was incorrect.

Response: The requirement in the final rule is covered by paragraph (b)(1)(vii) of FAR 52.204-21, which includes destruction as a possible sanitization technique. The URL for NIST 800-88 is not included in the final rule.

vi. Intrusion protection.

Comment: Several respondents commented on the requirement for intrusion protection in the proposed rule (FAR 52.204-21(b)(6)).

- One respondent stated that the only proposed intrusion-protection safeguards relate to malware protection services and security-relevant software upgrades. According to the respondent, these types of safeguards are generally not considered sufficient to provide a reasonable level of protection in a sophisticated enterprise environment.
- One respondent recommended that if hardware reaches its end of life and is no longer supported by the manufacturer, there should be a clause imposing a 6 month to 1 year deadline to upgrade the security system.

Response: The proposed requirements for intrusion protection have been replaced with paragraphs (b)(1)(xii)-(xiv) of FAR 52.204-21 to provide basic intrusion

protection. The recommendation for imposing a 6-month to 1-year deadline to upgrade the security system is outside the scope of this rule.

vii. Transfer limitations.

Comment: Various respondents commented on the transfer limitations in the proposed rule (FAR 52.204-21(b)(7)), which limited transfer of Federal contract information only to those subcontractors that both require the information for purposes of contract performance and provide at least the same level of security as specified in this clause. The primary concern of the respondents was whether the prime contractors might be held responsible for reviewing or approving a subcontractor's safeguards.

Response: This requirement has been deleted. The final rule no longer focuses on the safeguarding of information, but of information systems. The requirement to flow the clause down to subcontractors accomplishes the objectives of the rule to require safeguarding of covered contractor information systems at all tiers.

c. Other recommended requirements.

Comment: Some respondents recommended additional requirements for inclusion in the final rule:

- **Training.** One respondent recommended that contractor information security employees be required to obtain the

same levels of certification and training as provided in the DOD 8570 guidelines. Another respondent recommended security awareness training, as required by 44 U.S.C. 3544(b)(4).

- **Penetration or vulnerability testing, evaluation, and reporting.** Several respondents recommended a requirement for periodic testing of the effectiveness of information security policies in accordance with 44 U.S.C. 3544(c).
- **Detecting, reporting, and responding to security incidents.** One respondent stated that under FISMA it is mandatory for contractors to report security incidents to law enforcement if Federal contract information is resident on or passing through the contractor information system. This respondent also expressed concern about how personally identifiable information (PII) notifications would be properly made, without reporting requirements.
- **DFARS rule.** One respondent recommended that this FAR rule should include procedures similar to those in the draft DFARS rule 2011-D039, Safeguarding Unclassified DoD Information.

- **Encryption at rest.** One respondent recommended that data be stored in an encrypted manner, rather than encrypting exclusively for the purpose of transit.
- **Cyber security insurance.** One respondent also recommended requiring Government contractors to carry insurance that specifically covers the protection of intangible property such as data. Another respondent thought that the rule would already require small businesses to maintain cyber liability insurance.

Response: This rule establishes minimum standards for contractors' information systems that process, store, or transmit Federal contract information where the sensitivity/impact level of the Federal contract information being protected does not warrant a level of protection necessitating training, penetration or vulnerability testing, evaluation, and reporting, detecting, reporting, and responding to security incidents, encryption at rest, or cybersecurity insurance. Such standards would be needed if contract performance involved the contractor accessing CUI or classified Federal information systems. The final rule under DFARS Case 2011-D039, retitled "Safeguarding Unclassified Controlled Technical Information" (published in the Federal Register at 78 FR 69273 on November 18, 2013), provided for enhanced

levels of safeguarding because that case addressed a more sensitive level of information. Requiring cybersecurity insurance is outside the scope of this case.

d. Order of precedence.

Comment: One respondent commented on the order of precedence in the proposed rule at FAR 52.204-21(d), which stated that if any restrictions or authorizations in this clause are inconsistent with a requirement of any other such clause in the contract, the requirement of the other clause takes precedence over the requirements of this clause.

Response: The proposed paragraph at FAR 52.204-21(d) has been deleted from the final rule, and replaced by a new paragraph (b)(2). The basic safeguarding provisions should not conflict with any requirement for more stringent control if handling of more sensitive data is required. Paragraph (b)(2) of the FAR 52.204-21 clause states that there may be other safeguarding requirements for CUI.

e. Noncompliance consequences.

Comment: One respondent was concerned that any inadvertent release of information could be turned into not only an information security issue but also a potential breach of contract.

Response: The refocus of the final rule on the safeguarding requirements applicable to the system itself should allay the respondent's concerns. Generally, as long as the safeguards are in place, failure of the controls to adequately protect the information does not constitute a breach of contract.

3. Clause.

a. Prescription.

Comment: Several respondents commented on the prescription for use of clause 52.204-21.

- One respondent was concerned that it would be difficult to know when to use the clause because contracting officers have limited insight into offerors' existing information systems.
- One respondent recommended incorporating the clause into the list of clauses at FAR 52.212-5 instead of separately prescribing it at 12.301 for use in solicitations and contracts for the acquisition of commercial items.

Response: The clause is prescribed for inclusion in the solicitation when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system. This does not require any specific knowledge of the contractor's

existing information system. Generally, the person drafting the contract requirements/statement of work would know if contract performance will involve Federal contract information residing in or transiting through its information system. The contracting officer may not have the technical expertise to make this determination.

It is not possible to include FAR clause 52.204-21 in 52.212-5 because the clause is not necessary to implement statute or E.O.

b. Flowdown.

Comment: One respondent was concerned about the scope of the flowdown obligation, because it would be co-extensive with the definition of information. According to the respondent, the flowdown requirement would likely extend to all subcontracts for commercial items and COTS items, and even to small dollar value subcontracts.

Response: The clause only flows down to covered contractor information systems. The Councils have revised the final rule to exclude applicability to COTS items, at both the prime and subcontract level. However, there may be subcontracts for commercial items (especially services, e.g., a consultant) at lower dollar values that would involve covered contractor information systems. In such

instances, it is still necessary to apply basic safeguards to such covered contractor information system.

4. Acquisition planning.

Comment: One respondent was concerned that the acquisition planning requirement in the proposed rule at FAR 7.105(b)(18) could lead to varying security standards rather than uniform Governmentwide standards.

Response: The intent of the proposed requirement, which included a cross reference to the new subpart on basic safeguarding, was that the acquisition plan should address compliance with the requirements of the new subpart, not that each plan would invent a new set of requirements. The final rule has rewritten this requirement to make the requirement for compliance with FAR subpart 4.19 clearer.

5. Contract administration functions.

Comment: One respondent commented on the requirement in the proposed rule (FAR 42.302(a)(21)) regarding the contract administration function to "ensure that the contractor has protective measures in place, consistent with the requirements of the clause at 52.204-21." The respondent noted that the term "protective measures" was not used in the clause.

Response: This requirement has been deleted from the final rule.

6. Impact of rule.

Comment: Various respondents were concerned with the general impact of the rule and, in particular, the impact of the rule on small business concerns. One respondent stated disagreement with the Government's assessment that the cost of implementing the rule would be insignificant because it requires first-level protective matters that are typically employed as part of the routine course of doing business.

Some respondents were concerned that the lack of clarity imposes significant risks of disputes, and increases costs, since a contractor must design to the most stringent standard in an attempt to assure compliance. For example, several respondents were concerned that the potentially broad definition of "information" would significantly increase the compliance burden for contractors. Another respondent noted that the vagueness and subjective nature of some of the requirements (e.g., "best available" standard at 52.204-21(b)(2)) would place an incredible financial burden on businesses, creating an inequitable burden upon many small businesses.

Response: The final rule has been amended in response to the public comments (see section II.A. of this preamble), such that the particular requirements that were mentioned as imposing a greater burden have been clarified or deleted. As a result, the burden on all businesses, including small businesses, should not be significant.

IV. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under Section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

V. Regulatory Flexibility Act

DoD, GSA, and NASA have prepared a Final Regulatory Flexibility Analysis (FRFA) consistent with the Regulatory

Flexibility Act, 5 U.S.C. 601, et seq. The FRFA is summarized as follows:

> This action is being implemented to revise the Federal Acquisition Regulation (FAR) to safeguard contractor information systems that process, store, or transmit Federal contract information. The objective of this rule is to require contractors to employ basic security measures, as identified in the clause, for any covered contractor information system.
>
> Various respondents were concerned with the general impact of the rule and, in particular, the impact of the rule on small business concerns. The final rule has been amended in response to the public comments, such that the particular requirements that were mentioned as imposing a greater burden have been clarified or deleted. As a result, the burden on all businesses, including small businesses, should not be significant.
>
> This final rule applies to all Federal contractors and appropriate subcontractors, including those below the simplified acquisition threshold, if the contractor has Federal contract information residing in or transiting through its information system. The final rule is not applicable to the acquisition of commercially available off-the-shelf (COTS) items. In FY 2013, the Federal Government awarded over 250,000 contracts to almost 40,000 unique small business concerns. Of those awards, about half were for commercial items awarded to about 25,000 unique small business concerns. It is not known what percentage of those awards were for COTS items.
>
> There are no reporting or recordkeeping requirements associated with the rule. The other compliance requirements will not have a significant cost impact, since these are the basic safeguarding measures (e.g., updated virus protection, the latest security software patches, etc.). This final rule has basic safeguarding measures that are generally employed as part of the routine course of doing business. It is recognized that the cost of not using basic information technology system protection measures would be an enormous detriment to contractor and Government business, resulting in reduced system performance and the potential loss of valuable information. It is also recognized that prudent business practices to protect an information technology system are generally a common part of everyday operations. As a result, requiring basic safeguarding of contractor information systems, if

> Federal contract information resides in or transits through such systems, offers enormous value to contractors and the Government by reducing vulnerabilities to covered contractor information systems.
>
> There are no known significant alternatives to the rule that would further minimize any economic impact of the rule on small entities and still meet the objectives of the rule. DoD, GSA, and NASA considered excluding acquisitions below the simplified acquisition threshold, but rejected this alternative because there are many acquisitions below the simplified acquisition threshold where the Government nevertheless has a significant interest in requiring basic safeguarding of the contractor information system (e.g., a consulting contract with an individual).
>
> This final rule does not apply to the acquisition of COTS items, because it is unlikely that acquisitions of COTS items will involve Federal contract information residing in or transiting through the contractor information system. Excluding acquisitions of COTS items reduces the number of small entities to which the rule will apply.

Interested parties may obtain a copy of the FRFA from the Regulatory Secretariat Division. The Regulatory Secretariat Division has submitted a copy of the FRFA to the Chief Counsel for Advocacy of the Small Business Administration.

VI. Paperwork Reduction Act

The rule does not contain any information collection requirements that require the approval of the Office of Management and Budget under the Paperwork Reduction Act (44 U.S.C. chapter 35).

List of Subjects in 48 CFR Parts 4, 7, 12, and 52

Government procurement.

Dated: May 5, 2016.

William Clark,
Director,
Office of Government-wide
Acquisition Policy,
Office of Acquisition Policy,
Office of Government-wide Policy.

Therefore, DoD, GSA, and NASA amend 48 CFR parts 4, 7, 12, and 52 as set forth below:

1. The authority citation for 48 CFR parts 4, 7, 12, and 52 continues to read as follows:

Authority: 40 U.S.C. 121(c); 10 U.S.C. chapter 137; and 51 U.S.C. 20113.

PART 4—ADMINISTRATIVE MATTERS

2. Add subpart 4.19 to read as follows:

Subpart 4.19—Basic Safeguarding of Covered Contractor Information Systems

Sec.
4.1901 Definitions.
4.1902 Applicability.
4.1903 Contract clause.

Subpart 4.19–Basic Safeguarding of Covered Contractor Information Systems

4.1901 Definitions.

As used in this subpart-

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or

deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

4.1902 Applicability.

This subpart applies to all acquisitions, including acquisitions of commercial items other than commercially available off-the-shelf items, when a contractor's information system may contain Federal contract information.

4.1903 Contract clause.

The contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.

PART 7—ACQUISITION PLANNING

3. Amend section 7.105 by revising paragraph (b)(18) to read as follows:

7.105 Contents of written acquisition plans.

* * * * *

(b) * * *

(18) Security considerations. (i) For acquisitions dealing with classified matters, discuss how adequate security will be established, maintained, and monitored (see subpart 4.4).

(ii) For information technology acquisitions, discuss how agency information security requirements will be met.

(iii) For acquisitions requiring routine contractor physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system, discuss how agency requirements for

personal identity verification of contractors will be met (see subpart 4.13).

(iv) For acquisitions that may require Federal contract information to reside in or transit through contractor information systems, discuss compliance with subpart 4.19.

* * * * *

PART 12—ACQUISITION OF COMMERCIAL ITEMS

4. Amend section 12.301 by redesignating paragraphs (d)(3) through (7) as paragraphs (d)(4) through (8) and adding a new paragraph (d)(3) to read as follows:

12.301 Solicitation provisions and contract clauses for the acquisition of commercial items.

* * * * *

(d) * * *

(3) Insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts (except for acquisitions of COTS items), as prescribed in 4.1903.

* * * * *

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

5. Add section 52.204-21 to read as follows:

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

As prescribed in 4.1903, insert the following clause:

BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS
([INSERT ABBREVIATED MONTH AND YEAR 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER])

(a) Definitions. As used in this clause—

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures. (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

6. Amend section 52.213-4 by—

a. Revising the date of the clause and paragraph (a)(2)(viii);

b. Redesignating paragraphs (b)(2)(i) through (iv) as paragraphs (b)(2)(ii) through (v); and

c. Adding a new paragraph (b)(2)(i).

The revisions and addition read as follows:

52.213-4 Terms and Conditions—Simplified Acquisitions (Other Than Commercial Items).

* * * * *

TERMS AND CONDITIONS—SIMPLIFIED ACQUISITIONS (OTHER THAN COMMERCIAL ITEMS) **([INSERT ABBREVIATED MONTH AND YEAR 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER])**

(a) * * *

(2) * * *

(viii) 52.244-6, Subcontracts for Commercial Items **([INSERT ABBREVIATED MONTH AND YEAR 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]).**

* * * * *

(b) * * *

(2) * * *

(i) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems **([INSERT ABBREVIATED MONTH AND YEAR 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER])** (Applies to contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.

* * * * *

7. Amend section 52.244-6 by—

a. Revising the date of the clause and in paragraph (a) the definition "Commercial item";

b. Redesignating paragraphs (c)(1)(iii) through (xiv) as paragraphs (c)(1)(iv) through (xv); and

c. Adding a new paragraph (c)(1)(iii).

The revisions and addition read as follows:

52.244-6 Subcontracts for Commercial Items.

* * * * *

SUBCONTRACTS FOR COMMERCIAL ITEMS **([INSERT ABBREVIATED MONTH AND YEAR 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER])**

(a) * * *

Commercial item and commercially available off-the-shelf item have the meanings contained in Federal Acquisition Regulation 2.101, Definitions.

* * * * *

(c)(1) * * *

(iii) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems **([INSERT ABBREVIATED MONTH AND YEAR 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER])**, other than subcontracts for commercially available off-the-shelf items, if flow down is required in accordance with paragraph (c) of FAR clause 52.204-21.

* * * * *

BILLING CODE 6820-EP

[FR Doc. 2016-11001 Filed: 5/13/2016 8:45 am; Publication Date: 5/16/2016]